UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/773,866 | 02/07/2004 | Ryon K. Coleman | 03,123-A | 7225 |

32097 7590 04/23/2007

LESAVICH HIGH-TECH LAW GROUP, P.C.
SUITE 325
39 S. LASALLE STREET
CHICAGO, IL 60603

| EXAMINER | |
|---|---|
| PEACHES, RANDY | |
| ART UNIT | PAPER NUMBER |
| 2617 | |

| SHORTENED STATUTORY PERIOD OF RESPONSE | MAIL DATE | DELIVERY MODE |
|---|---|---|
| 3 MONTHS | 04/23/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/773,866 | COLEMAN ET AL. | |
| | Examiner | Art Unit | |
| | Randy Peaches | 2617 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *7,8,10-14,16,17,25-29,31,32,34,36 and 37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *19 and 21-23* is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☒ Claim(s) *15,18,30,33 and 35* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/21/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. ***Claims 7-8,10-14, 16, 25-29, 32, 34 and 36-37*** are rejected under 35 U.S.C. 102(e) as being anticipated by Rockwell (U.S. Patent Publication Number 2003/0027550 A1).

Regarding ***claim 7***, Rockwell discloses of a wireless network intrusion detection and prevention system, comprising:

- a plurality of intrusion detection sensors, which reads on claimed "monitor agent applications," installed on a plurality of wireless network devices for collecting wireless event data from a mobile, which reads on claimed "wireless," network, hereinafter referenced as wireless network. See paragraph [0032];
- a plurality of wireless access points for providing access to the wireless network for the plurality of wireless network devices. See paragraph [0023];
- a secure communications link, via 802.11x, for providing secure communications between the plurality of wireless network devices and other components of the

wireless network intrusion detection and prevention system. See paragraph [0023 and 0024];

- an airborne policy enforcement component (62)(see paragraph [0032], which reads on claimed "cooperative decision engine," for collecting wireless event data from the plurality of said intrusion detection sensors installed on the plurality of wireless network devices the plurality of wireless network devices and the plurality of wireless access points, for screening the wireless event data for normal events and abnormal events, for sending decision data to an airborne security manager (34)(see paragraph [0021]), which reads on claimed "response initiator adaptive feedback engine," based on processing of the normal event and abnormal events and for receiving state data from the said airborne security manager (34). See paragraph [0032];
- a state machine model, (see paragraph [0028]), which reads on claimed "fuzzy association engine," including an adaptive learning detection system for adaptively detecting abnormal events and preventing similar abnormal events based on wireless event data received from the cooperative decision engine. See paragraph [0026 and 0028}; and
- a said airborne security manager (34) for receiving decision data from the said airborne policy enforcement component (62), for sending state information to the said airborne policy enforcement component (62), which is incorporated in the said airborne security manager (34)(see paragraph [0034]), for sending response control information to a plurality of wireless access points through the said

802.11x link, and for maintaining a running mistrust level for the plurality of wireless network devices and the plurality of wireless access points on the wireless network. See paragraph [0034 and 0035].

Regarding ***claim 8***, according to ***claim 7***, Rockwell continues to disclose wherein the system of comprises a plurality of smart wireless antenna subsystems associated with the plurality of Wireless access points. See paragraph [0017 and 0018].

Regarding ***claim 10***, according to ***claim 7***, Rockwell continues to disclose wherein the said 802.11x link includes wireless encrypted communications. See paragraph [0023].

Regarding ***claim 11***, according to ***claim 7***, Rockwell continues to disclose wherein the said airborne policy enforcement component (62) includes a wireless event anomaly profiler, a normal wireless event profile database and a set of wireless event misuse rules. See paragraphs [0027-0029].

Regarding ***claim 12***, according to ***claim 7***, Rockwell continues to disclose wherein the said airborne security manager (34) sends alarms and wireless event log files to a network administrator, and receives manual control from the network administrator. See paragraph [0025].

Regarding ***claim 13***, according to ***claim 7***, Rockwell continues to disclose wherein the running mistrust level of the said airborne security manager (34) includes a plurality of mistrust levels and a plurality of associated response mechanisms, wherein each state is in the form of event /response. See paragraph [0027].

Regarding ***claim 14***, according to ***claim 13***, Rockwell continues to disclose wherein the plurality of response mechanisms include a plurality of security protection suites, wherein one of the security protection suits is an encryption method. See paragraph [0024].

Regarding ***claim 16***, according to ***claim 13***, Rockwell continues to disclose wherein the plurality of associated response mechanisms includes continuing normal operation, cycling between a plurality of security protection suites, switching radio frequency bands, or excluding a wireless network device or wireless access point from the wireless network and requesting re-authentication and re-login of the wireless network device or wireless access point on the wireless network. See paragraph [0034].

Regarding ***claim 25***, Rockwell discloses of a wireless network intrusion detection and prevention system, comprising:

- maintaining plural security intrusion events, which reads on claimed "mistrust levels," for a plurality of wireless signals for a plurality wireless network devices

and for a plurality of wireless access points on a wireless network by a wireless security system. See paragraph [0024];

- detecting a wireless signal for a wireless event for a selected wireless network device or selected wireless access point on a smart wireless antenna subsystem. See paragraph [0017];
- determining a mistrust level for the detected wireless signal via the wireless security system using decision data created on the wireless security system from the detected wireless signal from the smart wireless antenna subsystem. See paragraphs [0024-0025, 0032 and 0034];
- comparing the determined mistrust level to a mistrust level stored for the plural wireless signals for the plural wireless network devices and plural wireless access points. See paragraph [0034]; and
- applying a selected security response control from the wireless security system based on the determined mistrust level to selected wireless network device or wireless access point. See paragraph [0040 and 0033].

Regarding ***claim 26***, according to ***claim 25***, Rockwell continues to disclose a medium having stored therein instructions for causing a processor to execute the steps of the method. See FIGURE 5 and paragraph [0033].

Regarding ***claim 27***, according to ***claim 25***, Rockwell continues to disclose wherein the step of determining a mistrust level includes analyzing the detected wireless signal for normal wireless events and abnormal wireless events. See paragraph [0027].

Regarding ***claim 28***, according to ***claim 25***, Rockwell continues to disclose wherein the step of determining a mistrust level includes analyzing the detected wireless signal for normal wireless events and abnormal wireless events in association with an adaptive learning detection system that collects and analyzes normal wireless events and abnormal wireless events over a time period T using a terrestrial network, which reads on claimed "neural network," wherein the terrestrial network is associated to the said mobile network, that is adaptively and dynamically updated based on new detected wireless signals for normal wireless events and abnormal wireless events. See paragraph [0039].

Regarding ***claim 29***, according to ***claim 25***, Rockwell continues to disclose wherein the neural network includes a Back Propagation Neural Network with positive training created With new detected wireless signal data. See paragraph [0039].

Regarding ***claims 32 and 34***, according to ***claim 25***, Rockwell continues to disclose wherein the step of applying a selected security response control includes cycling among a plurality of security protection suites. See paragraph 0034.

Regarding ***claim 36***, according to ***claim 25***, Rockwell continues to disclose wherein the smart wireless antenna subsystem operates at physical layer in a wireless network infrastructure on the wireless network. See paragraphs [0017-0019].

Regarding ***claim 37*** according to ***claim 25***, Rockwell continues to disclose wherein the wireless security system operates at data-link layer or higher layers in a wireless network infrastructure on the wireless network. See paragraph [0024].

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. ***Claims 17 and 31*** are rejected under 35 U.S.C. 103(a) as being unpatentable over Rockwell (U.S. Patent Publication Number 2003/0027550 A1) in view of Aljadeff et al. (U.S. Patent Publication Number 2003/0232598 A1).

Regarding ***claims 17 and 31***, according to ***claims 7 and 25***, Rockwell fails to clearly teach wherein the decision data includes X, Y coordinates for a physical location of a monitor agent application, wireless network or device, wireless access point where an wireless anomaly event has been detected, a confidence level in the detected wireless

anomaly event, a type of wireless anomaly and a mistrust level decrement value from a security protection suite.

Aljadeff et al. teaches in paragraph [0018 and 0032], wherein direct distance measurement information is used in determining the physical location of the devices,

Therefore, at the time of the invention it would have been obvious to a person of ordinary skilled in the art to modify Rockwell in view of Aljadeff et al. in order to provide a means to determine the exact location of the device being monitored for the intrusion event.

***Allowable Subject Matter***

3. ***Claims 19 and 21-23*** are allowed.

Regarding ***claim 19***, the Examiner has determined that at this current stage of prosecution the claimed language found in the claim 19, i.e."... creating a wireless beamform and directing the wireless signal from the rouge wireless network device to a null area in the wireless signal pattern being transmitted by the wireless access point...," is allowable over the prior art of record.

4. ***Claims 15, 18, 30, 33 and 35*** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

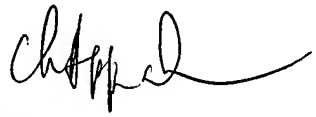
***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randy Peaches whose telephone number is (571) 272-7914. The examiner can normally be reached on Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph H. Feild can be reached on (571) 272-4090. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Randy Peaches
April 16, 2007



CHARLES N. APPIAH
SUPERVISORY PATENT EXAMINER